SecuAvail

［セキュアヴェイルニュース］

SECUAVAIL NEWS

セキュリティ運用監視サービスのセキュアヴェイルがお届けする、
情報セキュリティ向上に役立つフリーペーパー

Vol.12
2017.11

「SOC」誌上で「SOC」見学してみませんか？

誌上 SOC 見学
16年間の運用実態大公開!

セキュリティマネジメントサービスの歩み その2

SSL通信可視化専用機の取扱いを開始!

CONTENTS 01

セキュリティマネジメントサービスの歩み その2

NetStare Ver.1

2016年1月、セキュリティマネジメントサービス「NetStare」のVer.8をリリースしました。このコーナーでは、私たちのサービスの誕生からこれまでの歩みを世の中のセキュリティ動向とあわせてみていきたいと思います。

NetStare Ver.1スタート

2001年12月、NetStare Ver.1のサービス提供がスタートしました。
MSSP（※1）かつLAP（※2）である弊社は「お客様のセキュリティ情報部門」であるために、セキュリティでは早期の問題解決が必要だと考えています。そこでログの分析に注力し、MSSP+LAPをサービスの軸としました。LAPは現在のNetStareのログ分析の部分であり、MSSPは運用・監視サービスになります。セキュリティとシステムの可用性の両立が必要だという観点は、「Secure（安全）」と「Avail（可用性）」をかけた「SecuAvail」という社名の由来にもなっています。

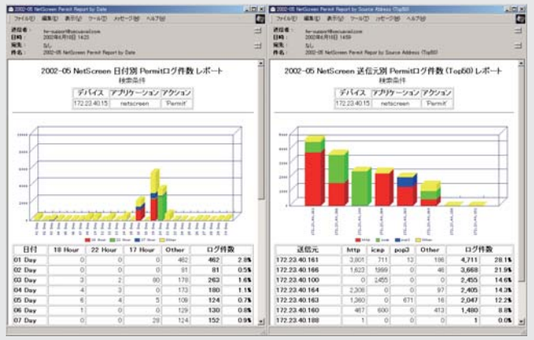
※1　MSSP:セキュリティ・サービス業者（managed security service provider）の意味ですが、セキュアヴェイルではmanaged security support providerという意味で使用しています。お客様のセキュリティをサポートする事業という想いが込められています。

※2　LAP:ログ分析事業（log analysis provider）の意味。

リリース当時のサービス

NetStareのリリース当時と現在で、サービスの軸は変わっていません。内容の変遷として1番に挙げられるのは、サービスの提供形態です。リリース当時、実はサービスの中身は全て手動で実現していました。機器の監視やログの分析からお客様へのレポート配信に至るまで、地道な手作業を重ねてNetStare Ver.1というサービスの形を成していました。
その後は徐々に作業の自動化が進みましたが、今でもセキュリティインシデントの対応アドバイスなどはお客様毎に手作業でご連絡しています。

Access Log Report サンプル（HTMLメール）



Illegal Attack Report サンプル

2002-05 Monthly IllegalAttack Report (ns5.secuavail.com) - 日本語 (自動選択)

ファイル(F)　編集(E)　表示(V)　ツール(T)　メッセージ(M)　ヘルプ(H)

送信者：　fw-support@secuavail.com
日時：　2002年6月20日 13:19
宛先：　なし
件名：　2002-05 Monthly IllegalAttack Report (ns5.secuavail.com)

2002-05 Illegal Attack Report

(ns5.secuavail.com)

日付	時間	メッセージID	不正アクセス	送信元アドレス	ポート	宛先アドレス	ポート	プロトコル	インタフェース
2002-06-19	20:20:46	system-alert-00011	ICMP Flood	192.168.1.211		192.168.1.241		1	untrust
2002-06-19	20:20:44	system-alert-00011	ICMP Flood	192.168.1.211		192.168.1.241		1	untrust
2002-06-19	20:20:42	system-alert-00011	ICMP Flood	192.168.1.211		192.168.1.241		1	untrust
2002-06-19	20:20:22	system-alert-00011	ICMP Flood	192.168.1.211		192.168.1.241		1	untrust
2002-06-19	20:20:19	system-alert-00011	ICMP Flood	192.168.1.211		192.168.1.241		1	untrust

CONTENTS 02

SSL通信可視化専用機のサービス化に向けて検証開始!

セキュアヴェイルからのお知らせ

SSL通信は暗号化されているため、セキュアに通信できることがメリットです。一方どのような通信なのか中身がわからないためIPS機能で遮断の判断ができないというデメリットもあります。そのため、SSL通信を一時的に復号化し、通信の中身をIPSで精査できるようにしたいというニーズは少なくありません。

そこで、セキュアヴェイルはSSL復号化専用機のサービス化検討のための検証を11月より開始します。専用機の導入により、SSL通信を復号化・暗号化する際の負荷をUTMにかけることなく通信の内容を精査することが可能になります。

「SSL」ってなに？

Secure Socket Layerの略で、データを暗号化する通信方法のことです。第三者による通信の盗聴や改ざんを防ぎます。ブラウザのアドレスバーに鍵のアイコンが表示されていたり、URLが「https」から始まる場合は、SSLによる暗号化通信が行われています。

検証予定機器のご紹介

F5：Herculon SSL Orchestrator

複数のセキュリティツールを一元に復号化・再暗号化!
リスクに応じた可視化のコントロールが可能。

MONITORAPP：APPLICATION INSIGHT SVA

SSLトラフィックの暗号化・復号化を最適化!
Webベースの直感的なユーザインターフェイスを備える。

CONTENTS 03

16年間の運用実態大公開！

誌上SOC見学

SOC（Security Operation Center）と聞いて皆さんはどのような印象をお持ちだろうか。
セキュリティの専門家集団、「人」が対応するため大人数で業務に従事している、セキュリティインシデントの分析を行う華々しい仕事、カッコいい基地のような場所で働いている、こんなイメージを持っている方が多くいるのではないかと思う。

しかし実際はセキュリティインシデントの発生は業務のごく一部にすぎず、機器の性能トラブルや設定変更業務を日々行っている。
今回はSOC業務の実態を特別に公開し、皆さんの疑問にお答えしていこう。

SOCで働く人

セキュアヴェイルSOCは現在約35名で運営している。意外と少ない、という声をよく耳にするが、少人数で24時間365日の対応を実現するための理由がある。それは自社開発の監視運用基盤「NetStare Manager」。
この「NetStare Manager」はネットワーク機器をマネジメントするために開発しており、機器の稼動監視、インシデント監視、顧客管理まで一元化することができる。運用に必要なノウハウを詰め込んでいるため少人数で質を保ったサービスの提供を可能としている。

24時間365日の対応を実現するために、組織をオペレーター、エンジニア、アナリストに分け、業務単位で体制を組んでいる。（図）
会社設立当初から24時間365日の業務を開始し、試行錯誤の結果、現在オペレーターは4チーム、2交代制の勤務体制としている。

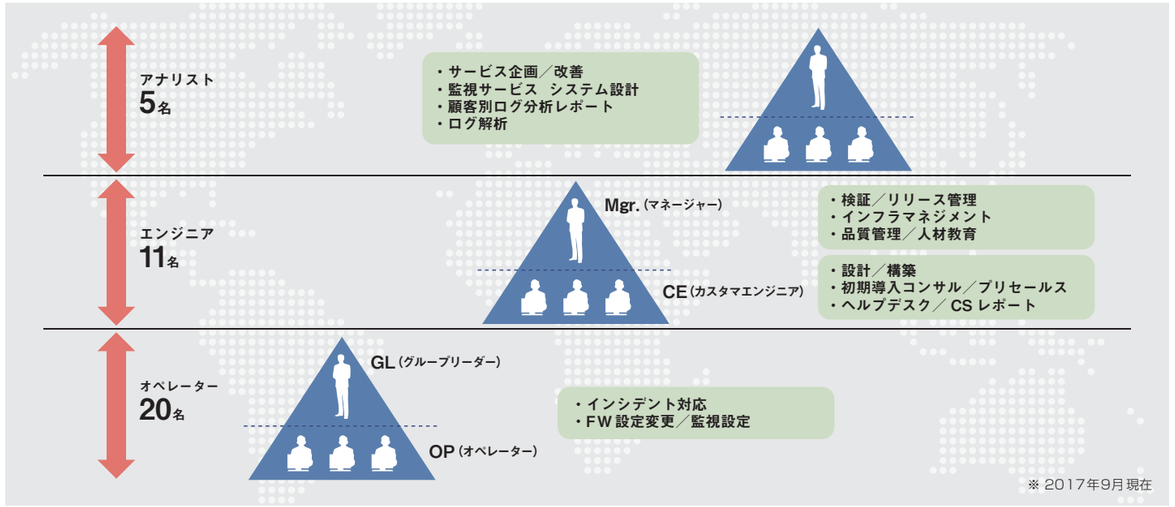


図　SOC 運用体制

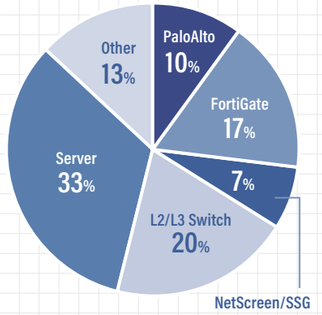
数字でみるセキュアヴェイルSOC

数字は嘘をつきません!正直なSOCの実態を知ってください。

顧客数
990社

監視対象デバイス数
2,700台

監視対象デバイス分類



ヘルプデスク問い合わせ件数
1日あたり
20〜40件
（新規問い合わせ）

設定変更件数
1日あたり
10件

インシデント件数
1日あたり
87件

IPSイベント件数
1日あたり
4〜10件

解析対象ログ件数
1日あたり
37億
3,500万件

分析対象ログ件数
1日あたり
2,880件

次回、SOCの業務内容をちょっとだけ公開します!

CONTENTS 04

本当に監視すべき兆候とは? - 二人三脚でログ分析に挑む -

【導入事例】ハウスビジネスパートナーズ株式会社さま

大手食品メーカー・ハウス食品グループの情報システムや会計、人事、総務業務を担う、ハウスビジネスパートナーズ株式会社さま(以下、同社)。セキュアヴェイルの運用監視サービスを導入いただき、ログ分析の強化をお手伝いさせていただいています。従業員数6,000人を超える著名ブランドのシステムを守る、同社システムソリューション事業部のお二方にお話を伺いました。

課 題

- ☑ 次世代ファイアウォールの自社運用は困難。
- ☑ 膨大なログからの取捨選択が必要。

成 果

- ☑ SOC アウトソースで工数削減。
- ☑ 本当に監視すべき脅威を絞り込み。

ブランドを守るためにも、セキュリティの強化が急務

同社が管理するサーバは約150台。その防御の要となっているのが、次世代型のファイアウォールです。

「以前は従来型のファイアウォールとウイルスソフトがセキュリティ対策の中心だったのですが、昨今は標的型メール攻撃が高度化し、情報漏えい事件も毎日のように報じられるようになっています。万一当社でも情報漏えい事件が起これば、社の信頼を失墜させブランドにも影響を及ぼしますので、そこはきっちりと防ぎたい」と語るのは、同社システムソリューション事業部次長・白石太郎さん。

「また、グループ全体でリスクマネジメントに取り組むなか、システムを受け持つ当社としてもきっちりとやっていきたかったんです」と、次世代型ファイアウォール導入に踏み切った理由を語ります。

しかし、次世代型ファイアウォールは、単に機械だけを導入しても、なかなか使いこなせるものではありません。機能が大幅に増える一方で、その性能を引き出すには経験とノウハウが必要だからです。必要なのは、一緒にセキュリティ強化に取り組めるパートナー。そこで同社が選んだのが、セキュアヴェイルでした。

ハウスビジネスパートナーズ株式会社

大阪府東大阪市

保険の代理店業および人事・経理・情報システム・総務業務の受託

システムソリューション事業部
次長　白石 太郎さん

システムソリューション事業部
グループマネージャー　石田 智也さん

24時間監視のみならず、対応のスピードも魅力

「選定に当たっては、もちろんコスト面もありますが、ネットワークの管理をお願いしているネットワークインテグレータさんと、きちんと連携してやっていただけることも重要でした」と、同社システムソリューション事業部グループマネージャー・石田智也さん。元々セキュアヴェイルを同社に紹介したのがこのネットワークインテグレータさまだったことや、次世代型ファイアウォールの導入検討中にセキュアヴェイルのログ分析サービスをご試用いただき、その内容をご評価いただけたことも、採用につながるきっかけとなりました。

当初ご採用いただいたのは、運用監視サービス「NetStare® for IDS/IPS」。次世代型ファイアウォールに搭載されているIPS(侵入防止装置)に特化したサービスです。
「IPSを導入するだけなら自社でできますが、運用は自社人員では難しい。そこをプロにやってもらうことで、24時間365日のログ監視体制を確立できました。こればかりは、実質自分たちでは無理ですから」(石田さん)。

「危険な兆候が見られたらすぐ通知をしてくれ、対策を取るかどうか、その場でエンジニアの方とのやり取りで決めてすぐ実行してもらえる。だから、工数が掛からない。導入の効果は出ていると思います」(同)。

最近では、オープンソース・ミドルウェアにまつわる深刻な脆弱性が明らかになり、それを狙った攻撃が続くこともありました。同社ではそのミドルウェアを使っていなかったので特に問題は起こらなかった反面、攻撃を警告する通知が頻発することに。「さすがに相談の上、その脆弱性に関係する通知を遮断しました(笑)」(同)

監視すべきログデータの取捨選択も共に

「NetStare® for IDS/IPS」でセキュアヴェイルのサービス力を実感していただいたことから、今はファイアウォール全体のログ分析もお任せいただいています。

「次世代型になってファイアウォール+IPSに加え、アプリケーションからのログも取れるようになり、ログ分析の重要性が増しました。それで今は、セキュアヴェイルの担当者の方と一緒に、ログの見方や、どの種類のログを監視していくかの取捨選択を行っています」(同)。

同社担当者さまとネットワークインテグレータの担当者さま、セキュアヴェイルの担当者の三者が、ログデータを見ながら協議を進める「報告会」は、真剣そのもの。「発生頻度ゼロのポリシーが多いと、そこがセキュリティホールになる恐れもあるので、整理していった方が良いです」「このアラートは、特定の取引先さんのサイトを見た時に出るもの。特に問題はありません」などと、実際のデータを元に、本当に監視すべき“ターゲット”を絞り込んでいきます。

「ログは精査していかないと、危険な通知に気付けなくなりますから」と石田さんは語ります。

“人”のセキュリティ強化もお手伝い

こうして、セキュリティ対策のレベルアップを重ねる同社。今後は、“人”にまつわるセキュリティの強化も進めたいといいます。

「機器の新規導入は、費用的にも限度があります。やはり、グループ内のセキュリティ教育が一番大事。ちょっと前までは、新聞で話題になった漏えい事件の手口などをグループ内に一斉通知したりしていましたが、グループ各社にはセキュリティ意識の強弱がそれぞれあるので、それを調べた上で今後は今まで以上にきめ細かく、濃淡を付けてやっていけないかと思っています。啓発活動を行っていく必要があると思います。また、eラーニングのコンテンツで、危機感が伝わるようなコンテンツのラインアップがあれば有難いですね」(白石さん)。

一方、石田さんは、知識レベルのさらなる向上も目指しています。
「先日、セキュアヴェイルのセキュリティセミナーに行きましたが、ああいう場所は知識が深まるので良いですね。」と仰っていただいています。

なるほど～ NetStare® ヘルプデスクを活用しよう！

お客様：「IPSにて不正アクセス検出のご報告」ってメールが大量に届いてるけど、なんだろう。
今度訪問にくるセキュアヴェイルの社員さんに聞けばいいのかな？

SA：NetStareサービスで監視対象となっている御社のIPSを通過した通信で、
危険度の高い内容を監視担当の者が確認し、コメントを付けてメールをお送りしています。

お客様：えっ？全部手作業でコメントを書いてくれているんだ。

SA：はい。御社の環境によって、何を確認すればいいのかなどの対応方法も書いています。

お客様：へえ、そうなんだ。コメントを確認して、システムが攻撃の影響の対象外のときは、
どうすればいいの？放っておけばいいのかな？

SA：システムに影響のない攻撃をログとして残すと、
本当に危険な攻撃のログと見分けがつきづらくなる場合があります。
また、ログが多くなってしまうのでUTM機器に負荷がかかり、機器の故障が早まる可能性があります。
ご覧になったメールに返信で「本シグネチャを「無効化」にしてください」と
一言書いて送っていただけますと、その攻撃によるログを取得しない設定を行えますよ。

お客様：じゃあ、攻撃の影響があるシステムの場合は？メールに書いてある対策をすればいいのかな。

SA：はい、その通りです。最初のうちはメールが多いかもしれませんが、
対応していただくことでIPSの設定がチューニングされてくるとメールも少なくなります。
もし内容について分からないことがあれば、そのまま返信で質問してくださいね。
ヘルプデスクの担当の者がすぐにお答えします。

お客様：なるほど!すぐに返信して尋ねればよかったんだね。

コラム「無知」と「無恥」

我々は日常、様々な言葉を用いて会話をする。言葉にはそれぞれ持っている意味がある。辞書で調べると意味を知ることはできるが、その言葉が人にもたらす印象や影響は、聞く側の人生観や経験により変わってくるのではなかろうか。先日、耳にしたことである。「営業力が不足しているので、売上目標を達成できないのです。」自らの行動で継続的に売上目標を達成する能力を営業力と定義するなら、確かにその能力不足が未達成の要因となるかもしれない。しかし、果たしてそうなのだろうか。20年以上営業職に携わった筆者には、このコメントに違和感を禁じ得ない。営業力の不足とは何を示唆しているのか？何をもってその力を身につけたとするのか？営業力という力を持っているから目標が達成できるのではなく継続して達成したという実績が、結果として営業力があると評価されるのではないだろうか。つまり、営業力があるから達成できるのではなく、達成の継続という実績そのものが営業力ではないだろうか。その力を養うために自らが行動し創意工夫の積み重ねをするしかないのである。人のフリを見ても力は養えるはずもなく、与えられるものでもない。目標達成に向けて能動的に周りが驚くほど行動する力。言い換えるならばこれを営業力と評しても良いではなかろうか。営業力不足という一言で未達成を説明することが、いかに恥ずかしいことか。知らないことは勉強で補えるが、恥ずかしいと思う気持ちが無い…無恥はどう解消したら良いのか…謙虚に顧客と向き合うことがまずは第一歩かもしれない。

SecuAvail

株式会社セキュアヴェイル（SecuAvail Inc.）
www.secuavail.com

大阪本社
〒530-0044　大阪府大阪市北区東天満1-1-19
アーバンエース東天満ビル
TEL:06-6136-0020　FAX：06-6136-0018

東京本部
〒104-0044　東京都中央区明石町8−1
聖路加タワー40階
TEL:03-6264-7180　FAX：03-6264-7181

発行 2017.11